ASIA CLEAN ENERGY FORUM 2026

Beyond Transition: Building Secure, Resilient, Inclusive, and Intelligent Energy Systems

8–11 June | ADB Headquarters, Metro Manila, Philippines

ADB

OT Cybersecurity

9 June 2026 | 4–5 p.m. (GMT+8)

In cooperation with

Ken Gau
Principal Industrial Consultant
kgau@dragos.com

DRAGOS

ABOUT THE SPEAKER

Ken Gau

Principal Industrial Consultant · Dragos

Twenty-five years across international IT operations and eleven years working OT cybersecurity in cybersecurity in Asia-Pacific oil & gas — downstream, upstream, operations, and capital project capital project design compliance.

BASED IN
Perth, Australia

SECTOR FOCUS
Oil & Gas · APAC

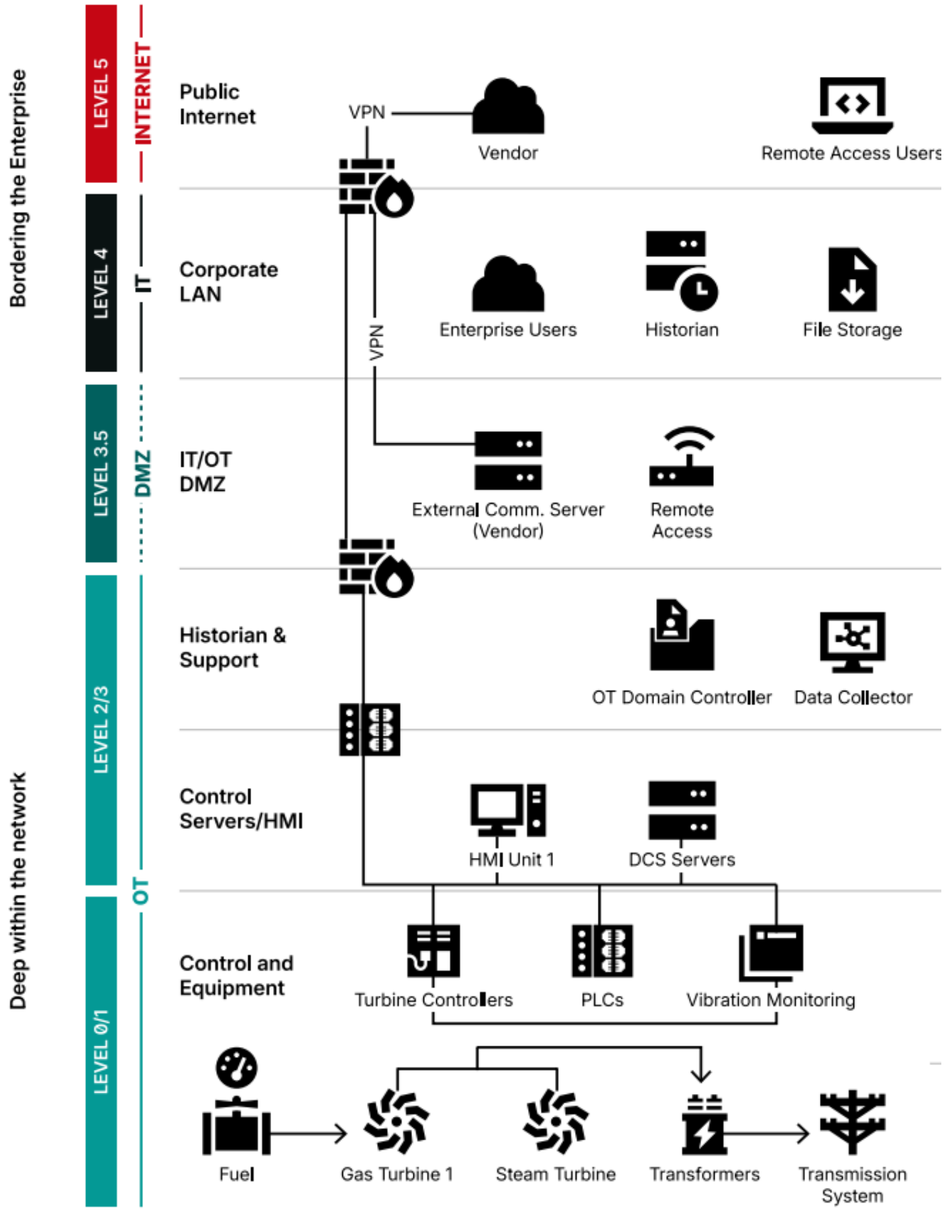
EXPERIENCE
25+ years IT · 11+ years OT

CERTIFICATIONS
CISSP · GICSP

OT / ICS SECURITY | ASIA-PACIFIC ENERGY | CAPITAL PROJECT DESIGN

BBA · ZICKLIN SCHOOL OF BUSINESS
BARUCH CITY UNIVERSITY OF NEW YORK

What “Cyber" Means in Clean Energy



DEFINITIONS, FIRST

What “Cyber" Means in Clean Energy

When ministers, lenders and project sponsors say "cyber risk," they usually mean three very different things. Clean energy systems sit at the systems sit at the junction of all three.

01 · PHYSICAL LAYER

Inverters, meters, batteries, wind & solar plant.

Hardware in the field. Anything with firmware and a network port is in scope — increasingly, that is everything. everything.

HARDWARE

02 · CONTROL LAYER

SCADA, EMS, DERMS, virtual power plants.

The software that turns intent into MW. This is where where attackers want to be — and where most lenders lenders never look.

SOFTWARE

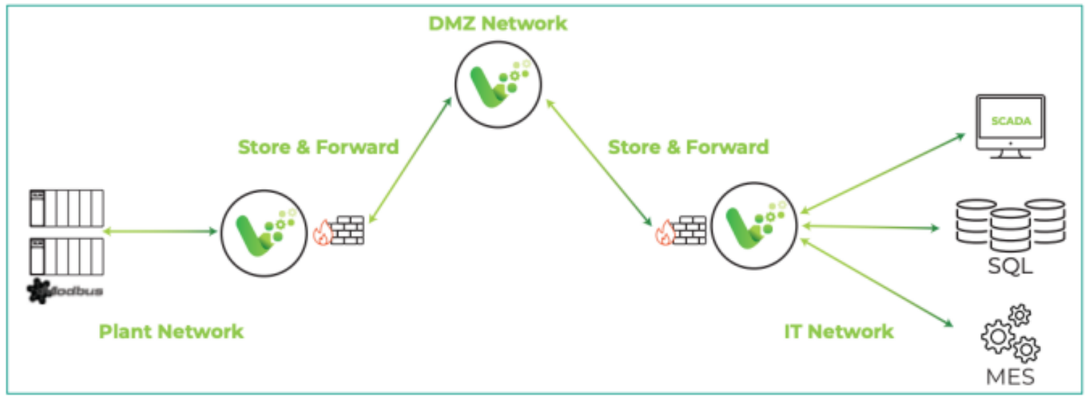
03 · BUSINESS LAYER

PPAs, settlements, market participation, comms.

The contracts and data flows that make a clean-energy clean-energy asset bankable. Cyber risk here shows up as up as revenue loss, not outage.

CONTRACTS

```
# ═══════════════════════════════════════════════════════════════
# COMANDOS PARA DETECTAR PROPÓSITO DEL SISTEMA
# ═══════════════════════════════════════════════════════════════

# Detección de propósito/rol del servidor
SYSTEM_PURPOSE = {
    # Hostname patterns
    "hostname_full": "hostname -f 2>/dev/null; hostname 2>/dev/null",

    # Qué aplicaciones corren
    "running_apps": "ps aux | grep -vE 'grep|ps aux' | awk '{print $11}' | sort | uniq -c | sort -rn | head -20",

    # Servicios activos
    "services_running": "systemctl list-units --type=service --state=running 2>/dev/null | grep -v 'UNIT' | head -25",

    # Puertos escuchando
    "listening_detailed": "ss -tlnp 2>/dev/null | grep LISTEN",

    # Tipo de aplicación web
    "web_apps": """
        ls -la /var/www/ /opt/*/webapps/ /opt/*/deploy/ /u01/*/domains/*/servers/*/tmp/_WL_user/ 2>/dev/null | head -30
    """,

    # Logs activos - qué tipo genera
    "log_types": "ls -la /var/log/*.log /opt/*/logs/*.log 2>/dev/null | head -15",

    # Bases de datos
    "db_detection": """
        ps aux | grep -iE 'oracle|mysql|postgres|mongo|redis|elastic|cassandra' | grep -v grep
        ls -la /var/lib/mysql /var/lib/pgsql /var/lib/mongodb /u01/app/oracle 2>/dev/null
```

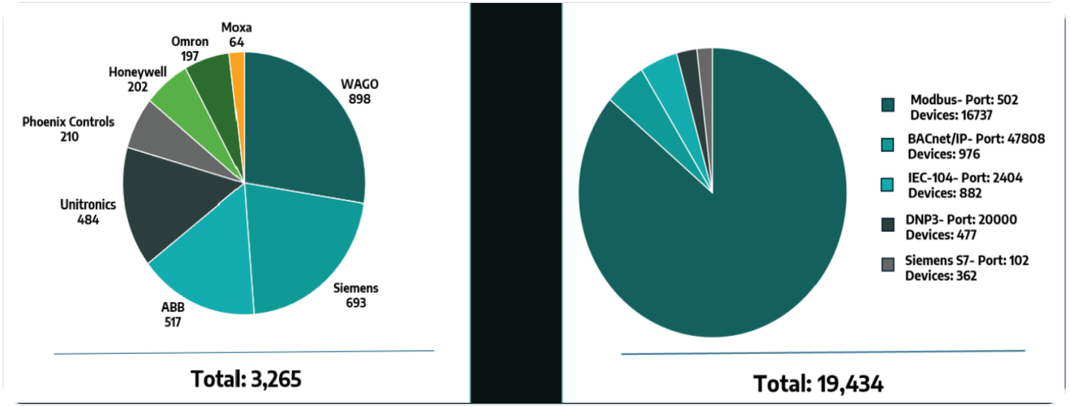


Why This Matters?

Servicios de Agua y Drenaje de Monterrey (Mexican Municipal Water & Drainage Utility)

Dec 2025 to Feb 2026

- Earlier this year, attackers tried to walk from the office network into the operational network of a water utility, using a public AI chatbot to help them find the boundary
- They never made it into operations because the operator had done two boring things: changed default passwords, and separated office systems from control systems.



Exposed devices by vendor and by protocol.

Country	Number of Exposed Devices
United Kingdom	5737
Germany	2377
Netherlands	1304
France	1288
Sweden	983

Top countries by exposed device count · Dragos 2026 assessment.

EUROPEAN EXAMPLE

Clean grids are digital grids

Inverters, smart meters, EV chargers, battery management, virtual power plants — every — every clean energy asset has a small computer in it, and most are reachable from a from a network.

19,000 +

EXPOSED ICS DEVICES

Industrial control devices reachable from the open internet in Europe alone — Dragos 2026 assessment.

THE CATEGORY

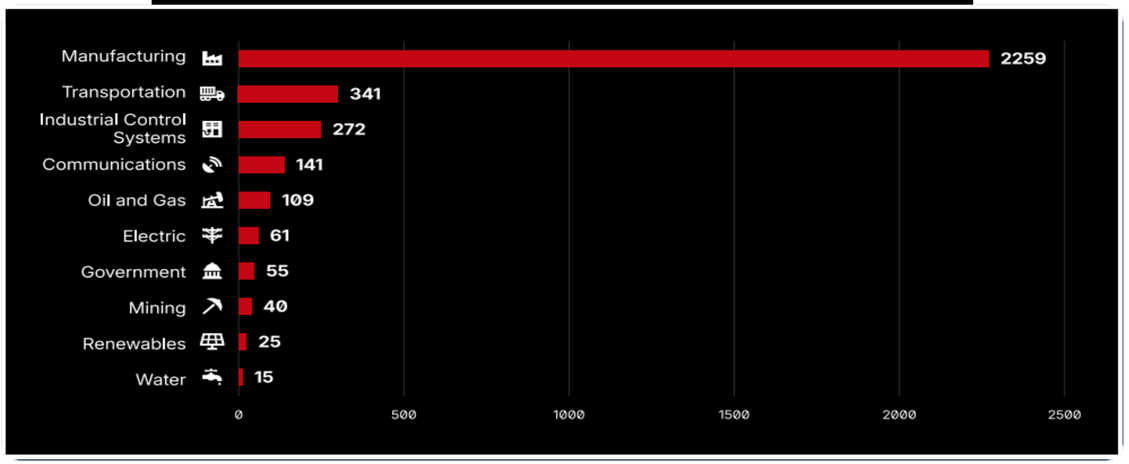
Exposed assets are configuration, not not capital.

Fixed with checklists and procurement language — not language — not new spend.

https://www.dragos.com/ot-cybersecurity-year-in-review

Q1 2026 · DRAGOS YEAR IN REVIEW

Disruption is now an everyday business cost.



Incidents by sector · Manufacturing carries the largest share; renewables & water are smaller but rising.

~1,020

INDUSTRIAL RANSOMWARE INCIDENTS

Recorded in Q1 2026 alone.

8 min

BETWEEN DISRUPTIONS

Roughly one industrial company is disrupted every eight minutes.

FOR A DEVELOPMENT BANK

A power purchase agreement, a project sponsor, a lender downtime risk is now also a now also a digital risk. Lenders are starting to expect to see it considered before close. before close.

https://www.dragos.com/ot-cybersecurity-year-in-review

SANS ICS CRITICAL CONTROLS

How do we fix this?

Five controls. Not new. Not glamorous. They define the ceiling on what attackers can actually break — and they're almost all almost all configuration, not capital.

ICS CRITICAL CONTROLS

01 **ICS Incident Response Plan**
Who picks up the phone at 3am when a PLC goes weird.

02 **Defensible Architecture**
Segmentation between IT, OT, and the wider operational estate.

03 **ICS Network Visibility & Monitoring**
You can't defend traffic you can't see — passive monitoring first.

04 **Secure Remote Access**
Vendor laptops, third-party support tunnels, MFA on every one.

05 **Risk-based Vulnerability Management**
Patch what matters in the right order — not every CVE by CVSS.

FOR THE ROOM

This is doable.

Five decisions any minister, financier, or project developer in the room can take.

01

Require cyber line items in project finance.

Treat it the way you treat insurance or insurance or HSE non-negotiable.

02

Add procurement language for OEMs.

No default credentials shipped. Disclosure obligations on vulnerabilities. vulnerabilities.

03

Demand secure architecture as a condition precedent.

Office network ≠ control network. Always.

04

Ask "who responds at 3 am?" before sign off.

An IR plan in writing names, numbers, numbers, escalation tree.

05

Report cyber risk in annual disclosures.

If it isn't measured publicly, it doesn't get doesn't get budget.

THE POINT

Most of the gap closes with checklists and procurement clauses not a single piece of new hardware.

THREE POINTS TO LEAVE WITH

Closing points.

01

Clean energy is a digital system.

Every clean energy asset has a computer in it. Cyber risk follows the kit.

02

The gap is configuration & policy, not capital.

Most of the risk closes through procurement and operations discipline.

03

Lenders, sponsors and ministers can set the bar.

If finance asks for it, the market delivers it. Default to required, not optional.

THANK YOU · ASIA CLEAN ENERGY FORUM 2026

Thank you.

Ken Gau

Principal Industrial Consultant · Dragos

kgau@dragos.com

DRAGOS

Scan to follow up or reach out after the session.